TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ

SOSYAL BİLİMLER ARAŞTIRMALARI DERGİSİ

*E-ISSN: 2564-680X (Online)*
*Kış Sayısı / Winter Issue*
*Aralık / December 2024*
*Muhammed Hayati TABAN (2024). "MANNING VAKASININ İSTİHBARATA KARŞI KOYMA AÇISINDAN ANALİZİ"*
*Muhammed Hayati TABAN (2024). "ANALYSIS OF THE MANNING CASE FROM A COUNTER INTELLIGENCE PERSPECTIVE"*
*Tokat Gaziosmanpaşa Üniversitesi Sosyal Bilimler Araştırmaları Dergisi. Aralık, s.95-109. / Tokat Gaziosmanpasa University The Journal of Social Sciences Research. Winter, p.95-109.*
*Alanı(Siyaset Bilimi ve Uluslararası İlişkiler Araştırma) / Field (Political Science and International Relations Research)*
*Doi Numarası / Doi Number: 10.48145/gopsbad.1443572*
*Geliş Tarihi / Received: 27.02.2024* *Kabul Tarihi / Accepted: 21.08.2024*

# MANNING VAKASININ İSTİHBARATA KARŞI KOYMA AÇISINDAN ANALİZİ

Muhammed Hayati TABAN[1*+]

[1]*Dr. Öğr. Üyesi, Millî Savunma Üniversitesi, Alparslan Savunma Bilimleri ve Millî Güvenlik Enstitüsü, İstihbarat Çalışmaları Anabilim Dalı, Ankara Türkiye / Turkish National Defence University, Alparslan Defence Sciences and National Security Institute, Intelligence Studies Department, Ankara, Türkiye,*
**mhtaban@kho.msu.edu.tr*
*[+]ORCID: 0000-0003-1785-9965*

***Öz–*** *2010 yılında Wikileaks aracılığıyla dünya tarihinin en büyük sızıntılarından biri yaşanmıştır. Amerikalı Er Bradley Manning askerî istihbarat analisti olarak Irak'ta görev yaparken yaklaşık 750.000 belgeyi Wikileaks'e sızdırmıştır. Er rütbesindeki bir askerî istihbarat personelinin bu büyüklükte bir sızıntıya yol açarken istihbarata karşı koyma açısından hangi ilkelerin çiğnendiği bu çalışmanın çıkış noktası olmuştur. Buradan hareketle bir iç tehdit olarak sınıflandırılabilecek Manning vakası istihbarata karşı koyma açısından alınması gereken dersler bakımından önem arz etmektedir. Bu çalışma Manning vakasını kendi kaleme aldığı otobiyografisinden (Readme.txt) hareketle asker olarak kaydolmadan önceki döneminden sızıntıların yaşandığı ana kadar İstihbarata Karşı Koyma açısından ve içerik analizi yöntemiyle analiz etmektedir. Çalışmada Prunckun'un İstihbarata Karşı Koyma teorileri temel alınmış ve analiz bu teorik çerçevede ve içerik analizi programıyla gerçekleştirilmiştir. Vaka üzerinden yapılan İstihbarata Karşı Koyma çalışmalarının teori ile pratiği birleştirilmesine ve örnek olaylar ile alınması gereken derslerin somutlaşmasına katkı sağlayacağına inancıyla gerçekleştirilen analiz sonucunda Er Manning'in askere alım sürecinden sızdırmayı gerçekleştrdiği döneme kadar olan süreçte neredeyse tüm İstihbarata Karşı Koyma ilkelerinin çiğnendiği ortaya konulmaktadır.*

***Anahtar Kelimeler–*** *İç tehdit, istihbarat, istihbarata karşı koyma, Manning, Wikileaks*

## ANALYSIS OF THE MANNING CASE FROM A COUNTER INTELLIGENCE PERSPECTIVE

***Abstract–*** *In 2010, one of the biggest leaks in world history unfolded through Wikileaks. While serving as a military intelligence analyst in Iraq, American Private Bradley Manning leaked approximately 750,000 documents to Wikileaks. The starting point of this study is to determine which principles of counterintelligence were violated by a military intelligence professional at the rank of private in causing a leak of this magnitude. From this point of view, the Manning case, which can be categorized as an internal threat, is important in terms of the lessons to be learned in terms of counterintelligence. This study analyzes the Manning case from her autobiography (Readme.txt), from the period before he enlisted as a soldier to the moment of the leaks, in terms of counter intelligence and through content analysis. The study is based on Prunckun's counter intelligence theories and the analysis is carried out within this theoretical framework and with a content analysis program. As a result of the analysis reveals that almost all Counter Intelligence principles were violated from the recruitment time of Private Manning to the time when he leaked the information, with the belief that counter intelligence studies based on case studies will contribute to combining theory and practice and concretizing the lessons to be learned with case studies.*

***Keywords –*** *Insider threat, intelligence, counterintelligence, Manning, Wikileaks*

## GİRİŞ

8 Şubat 2010 tarihinde ABD ve dünya tarihinin hacim ve içerdiği bilgiler açısından en büyük sızıntılarından biri yaşandı. Irak'ta askerî istihbarat analist olarak görev yapan Er Bradley (Chelsea) Manning yaklaşık 750.000 gizli belgeyi Wikileaks'e sızdırdı. Manning tarafından sızdırılan belgeler ("Irak Savaş Kayıtları", "Afgan Savaş Günlükleri" ve "ABD Diplomatik Yazışmaları") Nisan 2010 ve Nisan 2011 tarihleri arasında Wikileaks tarafından ifşa edildi. Bu belgeler The Guardian (Ball, 2011; Davies & Leigh, 2010; "WikiLeaks Embassy Cables: The Key Points at a Glance," 2010), Der Spiegel ("Explosive Leaks Provide Image of War from Those Fighting It," 2010; "Greatest Data Leak in US Military History," 2010; "WikiLeaks Diplomatic Cables," 2010), Le Monde ("Irak : L'horreur Ordinaire Révélée Par Wikileaks," 2010; "Wikileaks Évoque Des 'Preuves de Crimes de Guerre' Dans Les Rapports Sur l'Afghanistan," 2010; "WikiLeaks Publie l'intégralité Des 250 000 Câbles Diplomatiques Américains," 2011) ve El País ("La Verdad Sobre El 'Cablegate,'" 2010; "Las Dos Filtraciones Masivas Que Revelaron El Detalle Íntimo de La Guerra," 2010; "Los Crímenes de Irak Se Revelan al Mundo," 2010) gibi uluslararası gazetelerde haber oldu ve tüm dünya tarafından duyuldu.

O tarihten itibaren Wikileaks ve ABD hakkında çok sayıda akademik çalışma yayınlandı. Bu çalışmalar özellikle diplomatik sızıntıların ABD'nin dış politikasını anlamada birinci elden kaynaklar olarak değerlendirmiş ve bu amaçla sızıntıları analiz etmiştir (Hunt, 2019). Ayrıca bu sızıntılar Wikileaks'in şeffaflık açısından yeni bir çağ başlatıp başlatmadığı sorgulatmıştır (Roberts, 2012; Sifry, 2011). Yine bu doğrultuda sızıntılar Wikileaks'in ifade özgürlüğüne etkisi açısından ele alınmıştır (Ndeley, 2013). Manning sızıntılar sonrası Wikileaks, etik açıdan (Konstantopoulos, 2017; Randal, 2011) ve hukuki açıdan da çalışılmıştır (Bellia, 2012). İstihbarat çalışmaları alanında ise Wikileaks, istihbarat etiği çalışmalarına konu olmuş (Cole, 2022; Vrist Ronn, 2016), istihbarat paylaşımına etkisi açısından değerlendirilmiş (Montgomery, 2012), ve Manning vakası iç tehdit türlerinin sınıflandırılması açısından incelenmiştir (Hartline, 2017).

Fakat Manning vakası literatürde istihbarata karşı koyma (İKK) açısından henüz çalışılmamıştır. Bu nedenle Mart 2010'da yakalanan ve hapis cezası alan Manning'in sızıntıları istihbaratın temel unsurlarından olan istihbarata karşı koyma (Jensen, McElreath ve Melissa Graves, 2018:209; Johnson, 2010:6; Lowenthal, 2020:199) açısından bir vaka olarak ele alınmayı hak etmektedir. 7 yıl hapis yattıktan sonra ABD Başkanı Barack Obama tarafından affedilen Manning, 2022 yılında "Readme.txt" başlığıyla otobiyografisini yazarak yaptığı sızıntılara dair birinci elden bilgiler sunmuştur.

Bu vakada ilk olarak İKK açısından en önemli olan nokta, operasyonel bir ortamda görev yapan düşük rütbeli bir askerî istihbarat analistinin, çoğu stratejik olarak değerlendirilebilecek bu kadar geniş kapsamlı verilere nasıl erişim sağlamış olabileceği soruş öne çıkmaktadır. Bu verileri gizli bilgisayar sistemlerinden bu kadar büyük hacimlerde nasıl çıkardığı ve daha sonra bunları gizli bir alandan çıkarıp "bilgi sızdırmaya" adanmış olduğunu açıkça belirten bir organizasyonun eline nasıl ulaştırdığı İKK açısından anlaşılmaya değerdir. Böylesine büyük bir sızıntı hem ABD ordusuna hem de ABD çıkarlarına hacmi oranında zarar vermiştir. Nitekim dönemin ABD Savunma Bakanı Robert Gates de "Bu belgelerin yayınlanmasının savaş alanındaki sonuçları askerlerimiz, müttefiklerimiz ve Afgan ortaklarımız için potansiyel olarak ciddi ve tehlikelidir ve dünyanın bu kilit bölgesindeki ilişkilerimize ve itibarımıza zarar verebilir. İstihbarat kaynakları ve yöntemlerinin yanı sıra askeri taktikler, teknikler ve prosedürler de düşmanlarımız tarafından bilinir hale gelecektir."(Levine, 2010) diyerek durumun vahametine işaret etmiştir.

Böylesi sızıntıların devletlere verdiği zarar düşünüldüğünde büyük sızıntıların sadece stratejik düzeydeki istihbaratı etkileyebileceği sonucuna varmak yanlış olur. Operasyonel ve hatta taktik düzeydeki istihbarat, potansiyel olarak tehlikeye girebilmektedir. Örneğin Taliban, Afganistan'da Amerikalılarla işbirliği yapan kişilerin isimlerini bulmak için Manning tarafından sızdırılan Wikileaks savaş kayıtlarını incelediğini iddia etmiştir (Gioe, 2014:55).

Bu noktada ikinci soru ise böylesine devasa bir sızıntı gerçekleşmeden önce potansiyel bir iç tehdidin İKK birimi tarafından nasıl fark edilmediğidir. Orduya katılmadan önce ve orduya katıldıktan sonra kişilik ve kimlik sorunları yaşadığına dair işaretler olmasına rağmen Manning'e işiyle alakası olmayan gizli belgelere erişim izni verilmesi olayın İKK açısından bir diğer boyutudur. Örneğin, Manning'in askerliğe başvuru sürecinde geçmişindeki sorunları (madde kullanımı, psikoterapi görmesi, evsizlik geçmişi gibi) açıkça beyan etmiştir. Fakat bu süreçteki İKK ilkelerinin ihlalleri ve derhal harekete geçmemenin sonuçları Wikileaks olayını takip eden aylarca süren tartışmalarda kendini göstermiştir (Prunckun, 2019: 9).

Üçüncü olarak Manning vakası, istihbarat organizasyonu ve kültürü açısından ele alındığında ise bu vaka ABD sistemindeki geniş kapsamlı bilgi paylaşımı anlayışını sorgulatmıştır. Vakanın gerçekleştiği dönem bilgi paylaşımı o denli geniştir ki Orta Doğu'da görev yapan genç bir askerî istihbarat analisti olarak Manning, temel görevleriyle hiçbir ilgisi olmayan dünyanın dört bir yanından diplomatik yazışmalara erişebilmiştir. Bu erişim, özellikle 11 Eylül sonrası ABD istihbarat topluluğu sarkacının neredeyse körü körüne bilgi paylaşımı yönünde aldığı mesafeyi göstermektedir (Gioe, 2014: 51).

Yukarıdaki sorulardan hareketle bu çalışmanın amacı İKK ilkeleri açısından bir iç tehdit olarak nitelendirilebilecek Manning vakasını kendi beyanları üzerinden içerik analizi yöntemiyle analiz etmektir. Çünkü iç tehditlerin İKK açısından vaka temelli analizi İKK ilkelerinin öneminin ortaya konulmasına katkı sağlayacaktır. İç tehditler, savunma amaçlo İKK'nın odak noktalarından birisidir. İstihbarat tarihi (özellikle Soğuk Savaş dönemi) iç tehdit örnekleriyle doludur. Buradan hareketle çalışmada ilk olarak iç tehdit kavramı netleştirilecektir. Ardından İKK ve ilkeleri ele alınacak ve Hank Prunckun'un bu alandaki teorisi temelli

bir yapı oluşturulacaktır. İKK'nın personel güvenliği ilkesi açısından önemi nedeniyle Manning vakası asker olmadan önceki dönem, eğitim dönemi ve göreve başladığı dönem olmak üzere üç farklı dönemde İKK ilkeleri açısından analiz edilecektir.

Manning tarafından yazılan otobiyografinin ABD istihbarat topluluğu tarafından filtrelenerek, temizlenerek basımına izin verildiği hem Manning'in kitabın önsözündeki ifadelerinden hem de emekli ABD istihbarat topluluğu mensuplarının yazdığı kitap süreçlerinden bilinmektedir. Bu açıdan bu çalışmanın sınırlığı içerik açısından Manning'in otobiyografisi ile çizilmektedir. Bunun yanında kapsam açısından çalışmanın sınırlılığı ise istihbarata karşı koyma prensipleri ve özellikle iç tehditler ile belirlenmiş, inceleme askerî ve istihbarat topluluğu ile sınırlandırılmıştır. Çalışmanın yöntem açısından sınırlılığı ise içerik analizi manuel olarak İKK ilkeleri çerçevesinde gerçekleştirilecek olmasıdır.

## YÖNTEM

Manning vakasını analiz etmek için kendisi tarafından kaleme alınmış "Readme.txt" başlıklı otobiyografisi iki aşamalı şekilde içerik analizine tabi tutulacaktır. İlk aşamada güncel içerik analizi programlarından olan Masqda kullanılacaktır. Böylelikle otobiyografinin kelme bazlı analizi yapılacaktır. İkinci aşamada ise otobiyografi Prunckun (2019) tarafından geliştirilen İKK ilkeleri bağlamında incelenecektir. Bu ilkeler: Yönetim Sorumluluğu, Yönetim Desteği, Etik, Bilmesi Gerekenler, Bulunması Gerekenler, Keşfe Karşı Koyma, Gerçekçi Politikalar ve Prosedürler, Sinerjik Yaklaşım, Erken Tespit, Derinlikli Savunma, Öngörülemezlik, Korunması Gerekenler, Belirle ve Önceliklendir, Nitelik ve Nicelik, İşbirliği, Tehditleri Azaltma ve Yardıma Zorlama, Personel Güvenliği'dir. Bu temalar otobiyografide askere alınmadan önceki dönemi, eğitim dönemi ve asker olarak görev yaptığı dönem dikkate alınarak uygulanmıştır. Yakalandıktan sonraki dönem İKK açısından kapsam dışı olduğundan incelenmemiştir. İKK illelerini temalar olarak kullanıp Manning'in otobiyografisini bu şekilde analiz etmek İKK'nın hangi aşamalarda bir iç tehdidin engellenmesinde başarısızlığa uğradığını gösterme amacına hizmet edecektir.

## KAVRAMSAL ÇERÇEVE

### İç Tehditler

Vaka üzerinden iç tehdit-İKK ilişkisini kurmak amacıyla iç tehdit kavramının açıklanması elzemdir. İç tehdidi anlamak için öncelikle tehdit kavramını istihbarat bağlamına oturtmak gerekmektedir. İKK açısından bir tehdit unsuru değerlendirilirken, unsurun bir hedefe zarar verme niyetine ve kabiliyetine sahip olup olmadığı dikkate alınır. Tehdit unsurunun bu niyet ve kabiliyete sahip olup olmadığını belirlemek için analistlerin faktörlerin her biri için iki unsur belirlemeleri gerekir: Niyet için arzu ve beklenti (veya kabiliyet) ve kabiliyet için bilgi ve kaynaklar. Daha net ifade etmek gerekirse; tehdit = (arzu + beklenti) + (bilgi + kaynaklar). Niyet ve kabiliyet faktörlerini açacak olursak; arzu, tehdit unsurunun amacına ulaşmak için zarar verme isteği olarak tanımlanabilir. Beklenti, tehdit unsurunun planını gerçekleştirmesi halinde hedefine ulaşacağına dair duyduğu güvendir. Bilgi, tehdit unsurunun hedefine ulaşması için gerekli olan cihazları kullanmasını veya inşa etmesini ya da süreçleri yürütmesini sağlayacak bilgiye sahip olmasıdır. Kaynaklar, planlarını hayata geçirmek için gereken becerileri (veya deneyimi) ve bağlantıları içerir (Prunckun, 2019: 69).

Aktörler iç ve dış tehdit olarak ayrılırken rakipler (hasımlar); suçlular; ulus aşan teröristler; yerel teröristler; isyancılar ve gerillalar; anarşistler; siber suçlular; hak savunucuları; kiralık ajanlar (i.e., eski kolluk kuvvetleri gibi) ve yabancı istihbarat servisleri dış tehditleri kategorisine girmektedir. İç tehditlerin başında ise kurumun kendi çalışanları gelmektedir. Bu çalışanlar, mevcut yöneticiler, çalışanlar, eski çalışanlar, geçici çalışanlar ve taşeronlar olarak alt sınıflara ayrılabilir (Prunckun, 2019:73–74).

İstihbarat anlamıyla iç tehdit, bir kurumun varlıklarına/bilgilerine yetkili erişimi olan veya daha önce olmuş olan bir kişinin bu erişimini, kötü niyetli veya kasıtsız bir şekilde, kurumu veya ulusal güvenliği olumsuz yönde etkileyebilecek bir şekilde kullanma potansiyelidir (Common Sense Guide To Mitigating Insider Threats, 2022; Luckey et al., 2019: 15). Bu bağlamda iç tehdit, hükümet kurumlarındaki bilgilere erişim yetkisi olan bir kişinin bu yetkisini kasıtlı veya kasıtsız olarak kötüye kullanması veya suiistimal etmesiyle ortaya çıkar. İç tehdit, casusluk veya terörizm yoluyla; ulusal güvenlik bilgilerinin yetkisiz şekilde açığa çıkarılması veya kurum kaynaklarının/kabiliyetlerin kaybı veya zarar görmesi yoluyla zarar verebilir (The National Counterintelligence and Security Center, n.d.). Devletler açısından düşünüldüğünde iç tehditler büyük önem arz etmektedir. Tarihsel olarak devlet bilgi sistemleri her ne kadar çeşitli kaynaklardan gelen farklı tehditlerle karşı karşıya olsa da en büyük potansiyel tehdit bu sistemlere meşru erişimi olan içerden gelenlerden kaynaklanmıştır (Hayden, 1999: 1).

Hayden (1999) iç tehditleri niyetleri açısından ele alarak dört kategoride sınıflandırmaktadır:

Hain: Kuruma/devlete zarar verme, onu yok etme veya satma gibi kötü niyetli amaçları olan kişiler.

Fanatik: Kurumun/devletin belirli bir konuda doğru tarafta olmadığını düşünen veya bir konuda güçlü inanca sahip olan ve "kurumu düzeltmeye" çalışan içerden gelenleri içerir. Düzeltme yöntemleri yetkisiz bilgi sızdırma, veri tabanlarını yok etme veya dışarıdakilere veya diğer yetkisiz kişilere erişim sağlamayı içerebilir.

Bilgi meraklısı: Doğası gereği aşırı meraklı (genellikle "bilmesi gerekenler" ihlal eden) kişileri içerir.

İyi niyetli: Bilgisizlikten dolayı güvenlik ihlalleri yapanları kapsar. Paylaşımlı yazılım indirmek, virüs koruma yazılımını devre dışı bırakmak, onaylanmamış CD'ler kullanmak bir bilgisayar korsanının sisteme girmesi için ihtiyaç duyduğu yardımı sağlayabilir. İyi niyetli kullanıcı,

farkında olmadan suç ortağı haline gelir (Hayden, 1999: 2–4). Tüm bu kavramsallaştırma Manning vakasına uyarlandığında (özellikle Manning'in motivasyonları ve amaçları açısından) Manning fanatik bir iç tehdit olarak anlaşılmaktadır.

## TEORİK ÇERÇEVE

### İstihbarata Karşı Koyma

Manning vakasının otobiyografi üzerinden analiz edilmesi için İKK'nın teoril olarak anlaşılması gerekmektedir. Böylelikle hangi ilkelerin hangi aşamada ihlal edildiği ortaya konulacaktır. İKK teorisine yöneilk yapılan en kapsamlı çalışma Counterintelligence Theory and Practice (2009) eseri ile İKK'yı kapsamlı olarak ele alan ve ilkelerini net olarak ortaya koyan Hank Prunckun'a aittir. Bu nedenle Prunckun'un teorisi bu çalışmada benimsenmiştir.

İstihbarat üretim sürecinin temellerinden biri sırların yani gizli bilgilerin korunmasıdır. Bu amaçla İKK, öncelikle caydırıcılık ve tespit etmekle ilgilidir. İKK güvenlik odaklı bir işlevdir, ancak güvenlik değildir. Güvenlik İKK'da savunma amaçlı olarak kullanılır. İKK, bir kurumun istihbarat programını hasmın istihbarat servisine karşı korumayı amaçlayan bir faaliyettir. Kurum terimi burada herhangi bir örgüt, hatta bir ulus-devlet anlamında anlaşılmalıdır. Hasım terimi ise düşmanca niyetleri olan herhangi bir kişi ya da grup (ulus-devlet dahil) anlamında kullanılmaktadır (Prunckun, 2019: 41).

İKK'nın amacı; bir kurumu (ya da müşterisini) bir hasmın sızmasına karşı ve gizli bilgilerin yanlışlıkla sızmasına karşı korumak; casusluk, yıkıcı faaliyetler, sabotaj, terörizm ve diğer siyasi güdümlü şiddet biçimlerine karşı korumak; kilit teknolojilerin ve/veya ekipmanların transferine karşı tesislerini ve varlıklarını güvenli hale getirmek olarak sıralanabilir. Dolayısıyla İKK, savunmaya yönelik olduğu kadar saldırgan güvenlik yöntemlerine de başvuran ve istihbarat işlevinin özünü oluşturan araştırma ve analizleri kullanan aktif bir modeldir. İstihbarat ve İKK arasında net bir ayrım olsa da bu sınır çizgisi zaman zaman ince olabilmektedir. İKK işlevi aracılığıyla bir hasmın kendi kurumuna ya da dost kuruma sızma girişimleriyle ilgili olarak keşfedilen bilgiler istihbarat tarafını besleyebilir, rakibin bilgi boşluklarını ortaya çıkarabilir, yeteneklerini ve olası niyetlerini belirleyebilir. Dolayısıyla, İKK hem yürütülen bir faaliyet hem de karar vericileri bilgilendirmek için üretilen bir üründür (Prunckun, 2019:25).

Sırların korunmasındaki başarısızlığın geniş çaplı sonuçları vardır. İKK bu noktada devreye girmektedir. Ancak İKK gizli bilgileri saklamaktan daha fazlasıdır ve hassas bir dengede yürütülmelidir. Güvenliğe çok fazla önem verilmesi, analistlerin ve operasyon görevlilerinin ihtiyaç duydukları verilere erişememeleri ya da işlerini yapmalarını engellemesi nedeniyle görevin başarısızlığa uğramasına yol açabilir. Bu bağlamda İKK süreçleri, müttefik kurumlar ve hasım güçler arasında sürekli bir mücadeledir. Bu mücadelede İKK, istihbarat çalışmalarının entelektüel açıdan en zorlu alanlarından biridir (Prunckun, 2019: 3).

Bireyler, şirketler, ordu ve tüm uluslar güvenlik ve refahlarını İKK'ya borçludur denilebilir. İKK olmadan istihbarat işlevinin tüm tezahürleriyle bu kadar etkili olamayacağı kabul edilmelidir. Prunckun'a göre eğer espiyonaj bir spor olsaydı, İKK zanaatını icra edenler oyunun kalecileri olarak kabul edilmelidir. Bu uygulayıcılar olmasaydı, rakipler korunmasız kaleye atak yapma ve sonu gelmeyen goller atma konusunda tam yetkiye sahip olurlardı (Prunckun, 2019: 19).

İster bireyler, ister şirketler, ister ordu, isterse de tüm uluslar olsun, İKK'nın sağladığı koruma sayesinde bu kurumların güvenlikleri ve refahları artar. Bunun nedeni İKK'nın istihbarat işlevinin tüm tezahürlerini desteklemesi ve istihbaratın da sağlam ve rasyonel politikalar geliştirilmesini desteklemesidir. İKK olmasaydı, istihbarat kalesi saldırılara karşı sonuna kadar açık olurdu (Prunckun, 2019: 37–38).

### İKK İlkeleri

Mevcut literatür, çeşitli sektörler (kamu ve özel gibi) arasındaki farklılıklara rağmen, içeriden gelen tehditlerin sürekli değerlendirilmesine yönelik birçok uygulamanın tüm sektörlerde ortak olduğunu göstermektedir. Bu konuda Manning gibi iç tehditlerin İKK programından farklı değerlendirilmesi gerektiğine dair görüşler de vardır. Örneğin NATO Siber Savunma Mükemmeliyet Merkezi araştırmacıları İç Tehdit Programı (İTP) ile İKK Programını ayırmaktadır. Onlara göre İTP'ler, menşe ülkeleri ne olursa olsun, çalışanlarının neden olduğu olayları önlemek için yürütülür. Bu, bir ulusun kurumlarına yönelik casusluğun hükümetlerin İKK operasyonlarının ilgisini çekmediği anlamına gelmez; sadece hedef alınan kurumun içinde bir İTP kurulursa bu tür faaliyetlere karşı savunma ve kovuşturma yapma şansının daha yüksek olacağı anlamına gelir (Kont et al., 2015: 13).

RAND ekibi de iç tehditleri müstakil olarak değerlendirmekte ve iç tehditlerin önlenmesine yönelik ortak noktalara işaret ederek dört en iyi uygulama kategorisini ele almaktadır. İlk olarak ekip, kurumların neyin korunmaya değer olduğunun ve potansiyel tehditlerin tehlikeye atıcı davranış ve eylemlerinin belirlenmesine yardımcı olan risk değerlendirmesinin rolünü vurgulamaktadır. İkinci olarak, kurum içi tehditlere karşı bir koruma olarak kurum kültürünün rolünü ve bu kültürü teşvik etmek ve geliştirmek için periyodik eğitimlere vurgu yapmaktadırlar. Üçüncü olarak, en iyi tehdit izleme uygulamalarını önermektedirler. Son olarak ise güvenlik açıklarını azaltmak amacıyla içeriden kişilerin davranışlarını ve eylemlerini kontrol etmek için kullanılan ve sektör genelinde yürürlüğe konan bazı güçlü güvenlik politikaları incelemektedirler (Luckey et al., 2019: 23).

Daha önce bahsedildiği üzere istihbarat çalışmaları alanında İKK'yı teorik açıdan kapsamlı olarak ele alan ve ilkelerini net olarak ortaya koyan Hank Prunckun'dur. Pruncktun (2019) öncelikle İKK'yı yedi temel önermeye dayandırmaktadır. Bu önermeleri (ister istihbarat, ister yıkıcı faaliyetler, sabotaj, terörizm, silahların yayılması ya da rekabet avantajı için olsun) karşı tarafın bu verileri neden topladığına bakılmaksızın caydırma, tespit etme, aldatma ve

karşı tarafın bilgi toplama çabalarını etkisiz hale getirme kavramlarına dayandırmaktadır. Bu dört kavram Prunckun (2019) tarafından pasif savunma ve agresif savunma olarak sınıflandırılmaktadır. Bu iki kategori literatürde bazen önleme ve aldatma olarak da anılmaktadır. Savunma amaçlı İKK (yani önleme) caydırma ve tespit kavramlarını, saldırı amaçlı İKK (yani aldatma) ise aldatma ve etkisiz hale getirme kavramlarını kapsar (Prunckun, 2019: 42).

Prunckun'un İKK teorisi yedi önerme içermektedir (Prunckun, 2019: 43–46):

Önerme 1— Operasyonel Sürpriz

İKK'nın amacı diğer istihbarat işlevlerini desteklemektir, böylece bu işlevler operasyonel sürprizler gerçekleştirebilecektir. İKK bunu gizliliği tesis ederek ve koruyarak yapar.

Önerme 2—Veri Toplama

İkinci önerme, bir hasım gücün bir kurumun faaliyetleri hakkında veri toplamak için çeşitli araçlar kullanacağı varsayımına dayanır. Bu önerme aynı zamanda bir hasım tarafından kullanılan araçların veri toplamak için etik ve etik olmayan, yasal ve yasadışı olmak üzere mevcut tüm yolları içereceğini de göz önünde bulundurur.

Önerme 3—Mimleme

Hasım, veri toplama çabalarını bir kurumu ve onun işleyişini (ve kurumun korumaya hizmet ettiği varlıkları) ortaya çıkaracak bilgileri elde etmeye yönlendirecektir. Düşmanca bir bilgi toplama operasyonunun hedefi, bir kurumun yapısını (yasal ve anayasal yapısının yanı sıra emir komuta zinciri ve personeli), faaliyet ve etki alanını (örneğin coğrafi, ekonomik ve siyasi/sosyal), mevcut kabiliyetlerini (her açıdan) ve gelecekteki niyetlerini ortaya çıkaracak verilere odaklanacaktır.

Önerme 4—Kaynak

İKK, savunma operasyonlarını yürütmelerine olanak tanıyan personel ve kaynaklar olmadan gerçekleştirilemez.

Önerme 5—Kurgu Paradoksu

Savunma önlemleri, İKK'nın temel zorluğuna, yani bir istihbarat servisi ile hasım servis arasında oynanan zeka savaşına temel bir çerçeve sağlar. Bu mücadele kontrespiyonaj olarak adlandırılan saldırgan bir yaklaşım gerektirir. Bu tür operasyonlar, kurgu paradoksundan yararlanarak illüzyon yapabilen kurum personeli tarafından gerçekleştirilmelidir. Paradoks, bir kişinin algısını değiştirmeye dayanır, böylece gerçekte var olmadıkları halde gerçek olduklarına inanmalarına neden olan duygular yaşarlar. Böylelikle beynin gerçek olarak yorumladığı bir yanılsama ya da duyuların çarpıtılması gerçekleşir.

Önerme 6— Operasyonel Başarısızlıklar

Riskin tüm girişimlerin doğasında olması İKK operasyonları için de geçerlidir. Riskin olduğu yerde başarısızlık da vardır. Her ne kadar istihbarat başarısızlıkları basında ve sinema dünyasında dramatize edilmiş olsa da İKK başarısızlıkları diğer herhangi bir girişimdeki başarısızlıklardan farklı değildir. İKK başarısızlıkları yaşandığında -ki yaşanacaktır- bu olaylar bir kurumu felç etmemelidir. Kurumlar bu tür olaylara ve savunma önlemlerinin yeterliliğini gözden geçirmek için yenilenmiş bir gayretle karşılık vermeli, ancak yeni önlemlerin sorunsuz operasyonları engellememesine dikkat etmelidir. Savunma tedbirleri ile operasyonların iyi bir şekilde yürütülebilmesi arasındaki denge korunmalıdır. İyileştirici önlemler istihbarat personelinin görevlerini yerine getirmelerini asla engellememelidir..

Önerme 7—Analiz

İKK bir güvenlik işlevinden daha fazlasıdır ve özünde analiz vardır. İKK sanatı, gerçeklere ve akla dayalı politika seçenekleri ve operasyonel planlar üretmeden verimli veya etkili bir şekilde işleyemez. Mantıklı argüman analiz ile mümkün olur. Dolayısıyla, İKK uygulamalarının analitik çıktılara dayanması gerekir.

Prunckun (2019) ayrıca İKK'yı işlevleri açısından savunma ve agresif amaçlı olmak üzere iki alt türe ayırmaktadır. Prunckun (2019) Savunma Amaçlı İKK'yı caydırıcılık ve tespit üzerine inşa etmektedir. Caydırıcılık bir hasmın bilgiye erişimini engelleme yeteneğidir. Bu bağlamda caydırıcılık hem hasmı bir sızma operasyonu gerçekleştirme girişiminden vazgeçirme hem de bir sızma operasyonu başlatıldıktan sonra hasmın veri toplama operasyonunu engelleme becerisidir. Caydırıcılığın temelinde karşılanması gereken üç ilke vardır, aksi takdirde caydırıcılık başarısız olur. İlk ilke, kabul edilemez hasarla ilgilidir. Bir hasmın caydırılabilmesi için kendisine bir tür zarar verilebileceğini bilmesi gerekir. İKK bağlamında, caydırıcılık basitçe bir kurumun hasım kuvveti bir bilgi toplama operasyonu düzenlemenin maliyetlerinin veya risklerinin faydalarından daha ağır bastığına ikna etme yeteneğidir. İkinci ilke ise tehdidin hasım tarafından algılanması gerektiğidir. Eğer bir kurum hasmın etik olmayan ya da yasadışı veri toplamayı durdurmasını istiyorsa, hasmın böyle bir tehdidin gerçekten yapıldığını fark etmesi gerekir; tehdit iletilmezse hiçbir değeri olmaz. Üçüncü ilke ise inandırıcılıktır, tehdidin başarılı olabilmesi için inandırıcı olması gerekir. İnandırıcılık ise iki unsurdan oluşur; birincisi tehdidi yapan aktörün "kabul edilemez zararı" verebilecek kapasitede olması, ikincisi ise bunu yapabilecek iradeye sahip olmasıdır (Prunckun, 2019: 46–47).

Savunma amaçlı İKK'nın ikinci unsuru tespittir. Tespit, bir olayın gerçekleştiğini ve bu olayın bir şekilde gizli bilgilerin ihlali veya potansiyel ihlali ile ilişkili olduğunu fark etme eylemidir. Prunckun (2019) tespitin temelini oluşturan ilkeleri; endişe uyandıran bir olayın belirlenmesi; olaya karışan kişilerin tespit edilmesi; ilgili kişinin/kişilerin kurumsal ilişkisinin tanımlanması; ilgili kişinin/kişilerin mevcut konumunun belirlenmesi; ve kişi(ler)in olayı gerçekleştirdiğini gösteren olguların toplanması olarak sıralamaktadır. Bu tür olayları tespit edebilmek için, istihbarata karşı koyma personelinin bu olayları dikkatlerine sunacak sistemlere sahip olması gerekir. Sistemler, ofiste bu tür sorunları rapor etmek üzere eğitilmiş çalışanların gözlemlerini içerebilir ya da alarmlar veya insanların ofis içindeki faaliyetlerinin dijital görüntü kayıtları gibi teknik sistemler olabilir. Ne olursa olsun, sistemler olmadan tespit oranı azalır, olay fark edilmeyebilir, sonuçta hasmane operasyonun beklediği de budur (Prunckun, 2019: 47–48).

Bir olay tespit edilirse, failin de tespit edilmesi gerekir. Bu olmadan, ihlalin neden olduğu zararı değerlendirme olanağı azalır. Örneğin, bir İKK görevlisi verilerle kimin ilgilendiği, nasıl kullanılacağı ve bu "kayıp" bilgilerin kurum için ne gibi sonuçlar doğurabileceği konusunda güvenilir bir sonuca varamaz. İKK görevlileri yine de zararı ve hedeflenen amacı tahmin edebilir, ancak bu, kişinin kimliğini ve ihlali çevreleyen ayrıntıları bilmek kadar değerli olmayacaktır. İlgili kişinin tespit edilmesiyle yakından ilişkili olan, kişinin herhangi bir kuruluşla (hasım veya başka türlü) ilişkisinin tespit edilmesidir. Bir kişinin başka biriyle ya da başka bir örgütle ilişkisi olmadan sadece kendi başına hareket ettiğini düşünmek zor olacaktır. Casuslar veri toplar ve görevlerinin normal seyri içinde bu bilgileri merkezdeki istihbarat analistlerine aktarır, onlar da bu bilgileri analiz ve sentez ederek istihbarat raporları hazırlar. Böylesi bir olayda, örneğin kurumun (ya da müşterisinin) bazı işlerini "ifşa etmek" için tek taraflı olarak kişisel bir misyon üstlenen özel bir şahıs söz konusu olmadığı sürece, başka kimsenin dahil olmadığı bir durum düşünmek zordur. Ancak, böyle bir "görev adamı" durumunda bile, muhtemelen topladıkları bilgileri, zihinsel huzursuzluklarının özündeki hoş olmayan davranışı ifşa etmenin bir yolu olarak bazı yasal makamlara veya medyaya teslim edeceklerdir (Prunckun, 2019: 47–48). Prunckun (2019) Agresif İKK'yı ise aldatma ve etkisizleştirme üzerine inşa etmektedir. Aldatma, karşı tarafın karar vericilerini teşkilatın faaliyetlerinin, kabiliyetlerinin veya niyetlerinin (veya müşterisinin niyetlerinin) bazı yönleri hakkında yanıltmayı veya bir operasyonu kimin gerçekleştirdiğini gizlemeyi içerir. Burada nihai amaç, hasmın harekete geçmesini (ya da geçmemesini) sağlayacak bir görüş oluşturmasını ve böylece bu eylemlerin boşa çıkmasını sağlamaktır. Aldatma operasyonları kafa karışıklığına yol açarak hasmın etkili bir şekilde tepki vermesini geciktirmeyi ya da hasmın zamanını ve kaynaklarını boşa harcayacak bir yola girmesini sağlayacak yanlış bir anlayış yansıtmayı ve böylece kurumu eskisinden çok daha güçlü bir konuma getirmeyi amaçlayabilir. Etkisizleştirme ise bir hasmın istihbarat toplama operasyonunun engellenmesidir. Bir hasmın istihbarat toplama operasyonunda başarılı olabilmesi, başarılı olacağı varsayımına dayanır. Bu da hasmane operasyonların ya yok edilerek ya da durdurularak engellenebileceğini göstermektedir. Ayrıca operasyonun yürütülmesine (ya da bir operasyonun yürütülmeye devam edilmesine) yönelik ilgi ya da heves kaybına yol açarak ya da karşı tarafa güven kaybı yaşatarak da bu hedefe (tamamen ya da kısmen) ulaşılabilir (Prunckun, 2019: 49).

Manning vakası motivasyonu kendinden gelen, fanatik tipte bir iç tehdit olduğu için bu çalışmada Prunckun'un savunma amaçlı ilkeleri temel alınmıştır.

Bu ilkeleri Prunckun (2019) şu şekilde sıralamaktadır:

İlke 1— Yönetim Sorumluluğu

Savunma amaçlı İKK'nın ilkeleri arasında en üst sırada yer alan ilke icracı yönetişim ilkesidir. Her türlü güvenlik sorumluluğu kurumun/birimin başkanına/yöneticisine aittir.

İlke 2— Yönetim Desteği

Güvenliğin etkili olabilmesi için kurum yöneticisinin güvenliği teşvik etmeye istekli olması gerekir ki tüm çalışanlar bunu en olumlu şekilde anlasın ve kabul etsin. Kurum içindeki güvenlik imajı olumlu olmalıdır.

İlke 3—Etik

Güvenliğin kabulü için kilit konulardan biri, personelin güvenlik rejimini hakim sosyal normlarla uyumlu bir rejim olarak görmesidir; yani prosedürel uyumla başa çıkmak için baskıcı bir yönetim modelini yeniden yaratmaya çalışmamalıdır. etik olmayan karşı tedbirler uygulanmamalıdır.

İlke 4—Bulunması Gerekenler

Hassas bilgilerin işlendiği, analiz edildiği ya da depolandığı bir alana insanların erişimine izin vermenin gerekçesinin ortaya konması gerekir. Dostça erişim olarak bilinen bu yöntem, hasmın güç kullanmak yerine aldatma yoluyla erişim sağlamaya çalıştığı bir yöntemdir. Bu nedenle, bir kurumun ofislerine erişim, bilinen ya da randevusu olan çalışanlar ve ziyaretçilerle sınırlı olmalıdır.

İlke 5—Bilmesi Gerekenler

Savunma amaçlı İKK konusunda düşünülenlerin çoğu, eğer hasım hassas bilgilerin varlığından hiçbir zaman haberdar olmasaydı gereksiz olabilirdi. Bu da ilk güvenlik ihlalinin hasımın hedef alınmaya değer bir bilginin varlığından haberdar olmasıyla gerçekleştiği anlamına gelir. Bu noktada yapılabilecek tek şey savunma amaçlı İKK önlemlerini yoğunlaştırmak ve/veya saldırı amaçlı bir İKK operasyonu yürütmektir. Dolayısıyla, eğer bir kurum bir dereceye kadar hassas bilgilere sahipse, bu bilgilerin varlığının bilmesi gerekenler dışında herkese gizli tutulması gerekir.

İlke 6—Keşfe Karşı Koyma

Bu ilke, bilmesi gerekenler ilkesi ile ilişkilidir ve hasmın ilk etapta bilgi veya operasyondan haberdar olmasına izin vermemek anlamına gelir. Dolayısıyla bu ilke ile keşif yapılmasını engellenmesi amaçlanır.

İlke 7— Gerçekçi Politikalar ve Prosedürler

İKK amacıyla alınan karşı önlemlerin esnek olması ve riske karşılık gelmesi gerekir. Bunlar katı bir politika ve prosedürler dizisi haline gelmemelidir. Aksine, akıcı ve kurumun güvenlik gereksinimlerindeki değişikliklere uyarlanabilir olmalıdır.

İlke 8— Sinerjik Yaklaşım

İKK amacıyla alınan karşı önlemler modüler olmalı, İKK planlama sürecinin sonuçlarına bağlı olarak tamamen ya da kısmen uyarlanabilmelidir. Önemli olan, savunma amaçlı İKK ilkelerine uyulması ve uygulanan güvenlik standardını kontrol etmek için periyodik denetimlerin yapılmasıdır.

İlke 9— Erken Tespit

Hükümet kurumları ya da işletmeler için hırsızlık ve soygunlar alışılmadık bir durum değildir. Mini bir kale yaratmanın dışında, bir ofisi yüzde 100 hırsız geçirmez hale getirecek hiçbir şey yoktur. İdeal olarak bu ilke, İKK görevlisine sızma olayının gerçekleştiği anda bir uyarı gönderilmesini gerektirir.

İlke 10— Derinlikli Savunma

Erken tespit ilkesi, geciktirme ilkesinin ayrılmaz bir parçasıdır. Yani, bir kez tespit edildiğinde, karşı tedbirler faili geciktirmeye yönelik olmalıdır, böylece güvenlik

görevlileri veya polis gelip suçluyu yakalayabilir. Derinlemesine savunmanın ardındaki teori, faillerin her bir bariyerle karşılaştıkça ivme kaybedecekleri yönündedir. Tek bir savunma bariyeri olursa, aşılması zor olsa da, bir kez aşıldığında hedef veriler hemen savunmasız hale gelecektir. Bu durum tek bir hata noktası ya da hataya giden tek bir yol olarak bilinir. Bu ilke aynı zamanda, kurum için çalışan personelin sırları yanlışlıkla ifşa etmemesini sağlamak için bir tür "koruma" sağlanması gerektiğini belirtir.. Bu koruma, geçmiş araştırmaları biçimini alır. Her ne kadar fiziksel bir bariyer olmasa da sağlanan koruma yine de bir bariyerdir. Örneğin, gizli bilgileri kasıtlı olarak ifşa etmek isteyebilecek ve işe alınmaları halinde istemeden sırları ifşa edebilecek kadar patavatsız olabilecek kişilere karşı koruma sağlamak için bir inceleme sürecinin gerçekleştirilmesi gerekir.

İlke 11— Öngörülemezlik

Kurumun bariyer savunma sistemi, failin her bir bariyerle karşılaştığında irkilmesine veya kafasının karışmasına neden olacak bir özellik içerebilirse, bu durum bariyer sisteminin genel sağlamlığına katkıda bulunacaktır. Öngörülebilir bir bariyer, aşılmaya çalışıldığında birkaç olası sonucu olan bir bariyerden daha kolay aşılabilirdir.

İlke 12—Korunması Gerekenler

Derinlikli savunma ilkesinden hareketle, önemli ve hassas verilerin etrafında en güçlü bariyer kurulmalıdır. Ayrıca, bu tür verileri koruma riski de mümkün olan en küçük fiziksel profile indirilmelidir. Riskin geniş bir alana yayılması (örneğin, bir kurum binasının bir katı) bunu korumak için oluşturulan karşı önlemleri zayıflatabilir.

İlke 13—Belirle ve Önceliklendir

Savunma amaçlı İKK programının hassas bilgileri için sağlamlaştırma ihtiyacı varsa, önce bu öğelerin neler olduğu belirlenmelidir. Bu oldukça önemlidir ve İKK korumasına değer bilgi gruplarını belirlemek ve önceliklendirmek kaçınılmaz bir gerekliliktir.

İlke 14—Nitelik ve Nicelik

Hayatta birçok çaba içinde olduğu gibi, kalite miktar veya verimlilikten daha önemlidir. Bu durum savunma derinliği konusunda da aynıdır. Bu özellikle sistemdeki insanları içeren unsurlar söz konusu olduğunda ortaya çıkar. Bu bağlamda güvenlik görevlileri akla gelir. İyi eğitilmiş ve motive olmuş birkaç güvenlik görevlisi, görevlerini iyi bir şekilde yerine getirirken çok sayıda ancak kötü eğitilmiş ve isteksiz nöbetçilerden daha değerlidir.

İlke 15—İş birliği

Güvenlik genellikle kurumlara göre değişiklik gösterebildiğinden, bu ilke, İKK personeli ile harici yasal yürütme kurumları arasında iş birliğine ihtiyaç olduğunu belirtir. Bu, polisle ve suç önleme stratejilerine sahip benzer kurumlarla iş birliği yapmayı içerir; aynı zamanda gözaltına alınmaları ve davaların mahkemelerde yürütülmesi için yasal kurumlara resmî bir bağımlılığı içerir.

İlke 16 ve 17—Tehditleri Azaltma ve Yardıma Zorlama

Son olarak, başlangıçta birbirini tamamlayan gibi görünen ancak aynı zamanda birbirini dışlayan iki temel ilke bulunmaktadır. İlke 16, güvenlik stratejilerinin şüpheli faillerin listesini mümkün olan en küçük havuza indirebilme yeteneğine sahip olması gerektiğini belirtir. Bunun yapılabilmesi bir caydırıcı olarak görev yapar ve tespit olacağına dair bir sinyal verir. Ancak, güvenlik karşı önlemleri, korumaları ihlal etme yeteneğine sahip tek bir kişinin olmasını engellemek üzere tasarlanabilirse, bu, hassas veri elde etme girişimlerinde birden fazla kişinin yer almasını gerektirir. Bu da güvenlik önlemlerini aşmanın iki veya daha fazla kişiyi gerektireceğini sağlar (Prunckun, 2019: 53–62).

Prunckun (2019) İKK ilkelerinden ayrı ama bu ilkeleri tamamlayıcı olacak şekilde Personel Güvenliği'ni de ele almaktadır. Personel güvenliği ile ilgili merkezi prensip şudur: Kurum için çalışan personelin, kazara sırları ifşa etmemesini, kasıtlı olarak gizli bilgileri açıklamamasını veya (aşırı durumlarda) bu bilgileri kurumun tesisleri, süreçleri veya personeli aleyhine şiddet eylemlerinde kullanmamasını sağlamak. Personel güvenliği doğrudan kontrolle ilgili değildir, bilgi üreten veya bilgiyi kullanarak kararlar alan personelin yönetimi ile de ilgilidir. Bu süreç, kötü işe alma uygulamalarının önlenmesini de içerir. Çalışanların gizli bilgileri açıklamasına yol açabilecek uygulamalar ve hasım tarafından gerçekleştirilebilecek herhangi bir sızma girişiminin engellenmesi personel güvenliğinin merkezinde yer alır (Prunckun, 2019: 113).

Prunckun'un (2019) personel güvenliği ile doğrudan ilişkilendirdiği bir diğer İKK ilkesi İşe Alma Uygulamaları'dır. Güvenlik izni olan personel gerektiren pozisyonlar gizli veri üreten, kullanan veya işleyen pozisyonlardır. Örneğin istihbarat analistleri, gizli raporlar üretirler ve bu süreçte gizli bilgileri kullanırlar, dolayısıyla güvenlik izinlerine ihtiyaçları vardır. Yöneticiler, politika yapıcılar ve karar alıcılar gizli raporları kullanırlar, dolayısıyla onların da güvenlik iznine ihtiyaçları vardır. Liste uzundur ancak gizli verilere erişimi olan herkesin güvenlik izni alması gerektiğini söylemek yeterlidir (Prunckun, 2019: 114).

Personel güvenliği işe alım sürecinin ilk aşamasında başlar. Personel tahkikat süreci başvuru aşamasında başvuru sahibinin bir kişisel geçmiş beyanı doldurmasıyla başlamalıdır. Bunun arkasındaki mantık, İKK personeline, kişinin iddia ettiği kişi olduğunu ve gizlilikleri korumak için gerekli kişisel dürüstlüğe sahip olduğunu doğrulamak için yeterli bilgi sağlamaktır. Başvuru sahibinin tam adı, mevcut ikamet ve iş adresi ile doğum tarihi ve yerine ek olarak, kişisel geçmiş beyanı, ikamet geçmişi, eğitim bilgileri, medeni hali, vatandaşlık bilgileri, geçmiş iş bilgileri, askerlik ile ilgili bilgiler, finans ve kredi bilgileri, ve adli sicil gibi alt bilgileri de içerebilir. Bu süreçte arşiv araştırması, güvenlik izinleri için altın standarttır. Arşiv araştırması bir başvuru sahibinin kimliğini ortaya çıkarmak ve ifşa olması halinde kurumu veya devleti olumsuz etkileyebilecek gizli bilgileri güvenilir bir şekilde tutma kabiliyetini belirlemek için yapılır. Arşiv araştırması, kişinin kim olduğunu ve olgun, sorumlu, anlayışlı, dürüst ve sadık olup olmadığını belirlemeye yardımcı olur. Personel tahkikatında dört faktöre odaklanılır. Bunlar insanların sırlara ihanet etmesinde etkili

olan dört motivasyon olan para, ideoloji, taviz (yani kişinin şantaja uğramış olması) ve egodur (Prunckun, 2019: 115).
Ayrıca bir çalışan terfi ettiğinde veya hassas görevlere atandığında, tekrar bir inceleme prosedürü yürütülmelidir. Bu inceleme süreci, çalışanın ilk işe alınmasından bugüne kadar geçen süreyi kapsamalıdır. Bunun amacı, terfi eden kişinin yakın geçmişindeki herhangi bir faktörün, kullanacağı bilgilerin gizliliğini tehlikeye atıp atmayacağını tespit etmektir Bir arşiv araştırması yürütürken, İKK soruşturmacısı bir kişiyi "yakalamak" için tek bir ihlal ya da münferit bir muhakeme hatasına değil, kişinin muhtemelen istikrarsız, yani güvenilir olmayan ve sadakatsiz olduğuna dair net bir resim sunan faktörlerin bir kombinasyonuna bakar (Prunckun, 2019: 114–115). Prunkcun'un savunma amaçlı İKK teorisi bu çalışma için inceleme temalarımızı vermektedir. Bu temalar Yönetim Sorumluluğu, Yönetim Desteği, Etik, Bulunması Gerekenler, Bilmesi Gerekenler, Keşfe Karşı Koyma, Gerçekçi Politikalar ve Prosedürler, Sinerjik Yaklaşı, Erken Tespit, Derinlikli Savunma, Öngörülemezlik, Korunması Gerekenler, Belirle ve Önceliklendir, Nitelik ve Nicelik, İş birliği, Tehditleri Azaltma ve Yardıma Zorlama ve Personel Güvenliği'dir.

## İKK VE BRADLEY (CHELSEA) MANNING VAKASI

Bu çalışma Manning'i bir iç tehdit olarak kabul etmekte, yaptığı eylemin istihbarat ve güvenlik açısından yol açtığı sonuçlardan hareketle bir sonuca varmayı hedeflemektedir. Manning ve Manning gibilerin yaptıkları "leaking" (sızdırma) ve "whistleblowing" (ihbar etme) kelimeleri ile tanımlanabilmektedir. Bu iki farklı kullanım içerdikleri anlam açısından birbirinden farklı şeyleri çağrıştırmaktadır. Her ne kadar Manning'in nasıl tanımlanması gerektiği bu çalışmanın kapsamı dışında olsa da iki kullanımın netleştirilmesi gereklidir. Sızdırma (leaking), bilginin açıklanmaması gerektiğini ve sızdıran kişinin kötü niyetli bir amaca sahip olduğunu ima eder. Öte yandan, ihbarcılık (whistleblowing), yasal olarak korunan ve/veya etik açıdan haklı görülen, bir yanlışlığı ortaya çıkarmak amacıyla yapılan bir bilgi paylaşımıdır (Entman et al., 2009). İhbarcılar (whistleblowers) genellikle olumlu bir bakış açısını yansıtır. Yani, ihbarcılar gizli bilgileri kamuoyunun ilgisini algılanan bir yanlışlığa, suç veya adaletsizliğe yönlendirmenin gerekli olduğuna inanarak basına sızdıran kişi olarak görülürler (Thorsen et al., 2013: 102).
Dijital iletişim teknolojileri, ihbarcılığa başka bir karmaşıklık katmanı eklemiştir. Bilgi sızdırma ve yayma fiziksel eylemi kolaylaşmakla kalmamış, internet aynı zamanda bu olanakları katlamıştır. Bu sayede, ihbarcılar geleneksel medya kuruluşlarının yardımı olmadan ihbarda bulunma yeteneği kazanmışlardır (Thorsen et al., 2013:. 104). Manning de işte böyle bir dönemde eylemini gerçekleştirmiş ve İKK açısından ders alınması gereken bir vaka olarak tarihte yerini almıştır. Bu noktada Manning vakası otobiyografiye dayanarak asker olmadan önce-askere alınma süreci; sınıf eğitimi dönemi; ve istihbarat analisti olarak görev yaptığı dönem olarak 3 dönemde ele alınmaktadır.

### Asker Olmadan Önce ve Askere Alınma Süreci

İKK ilkeleri işe alım dönemindeki yapılması gereken arşiv araştırması sürecini de kapsadığı için Manning vakasının analizi kendisi tarafından yazılmış otobiyografisi (Readme.txt) temel alınarak asker olmadan önceki yaşamının anlaşılması gerekmektedir. Bu analize nedenle Manning'in askerlikten önceki yaşamından başlanmıştır.
Bradley Manning 1987 yılında Crescent, Oklahoma'da İrlanda kökenli Amerikalı bir ailede ablası Casey'dan sonra ikinci çocuk olarak doğmuştur. Babası, Brian Edward Manning, Vietnam Savaşı döneminde askere yazılmış ve deniz kuvvetlerinde analist olarak görev yapmış ve kendisi gibi gizli belgelerle çalışmıştır. Manning, ailevi sıkıntıları olan bir ailede alkol bağımlısı ebeveynlerin sorunları arasında genellikle ablası tarafından büyütülmüştür. Bu nedenle küçük yaştan ablası Casey'e özenmiş ve onun elbiselerini, makyaj malzemelerini ve eşyalarını kullanmayı istemiştir. Babasının bu konudaki sert tutumu nedeniyle 6 yaşından itibaren içine kapanmış ve bilgisayar ile vakit geçirmeye başlamıştır. Böylelikle kodlama ile erken yaşta tanışmış 10 yaşında kendi basit oyununu tasarlar duruma gelmiştir. Babasından gördüğü şiddet ve zorbalık nedeniyle ailesinden ihtiyacı olan şefkati ve ilgiyi görememiştir. Bu nedenle internette zaman geçirmeye başlamış ve hack forumları, ücretsiz yazılımlar, aktivistlere ilgisi artmıştır. 14 yaşında anne babası boşanmış ve Manning annesiyle Galler'e taşınmış ve orada yaşamaya başlamıştır (Manning, 2022: 20–30).
Manning Galler'de kaldığı sürede de yazılım yeteneklerini geliştirmiş, hack gruplarına katılmış ve web sitelerinin hacklenmesi ve serverlara saldırılması ve hatta yerel bir figürün ofisine girip hard diskinin kopyalanması gibi eylemlerde bulunmuştur. Manning küçük yaşta gerçekleştirdiği bu eylemlerindeki motivasyonunu "bilginin özgür olması gerekliliğine olan ideolojik inancı" ile açıklamaktadır (Manning, 2022: 35).
Buraya kadar anlattıkları Manning'in fanatik bir iç tehdit olarak anlaşılması açısından önemlidir. Nitekim bu dönemde bilgi çalma girişimlerine yönelmiş ve yasa dışı eylemlerde bulunmuştur. Nitekim Galler'de liseyi bitirdikten sonra yaptığı ilk şeylerden biri Myspace adresinde cinsel kimliğini açıklamak olmuştur. Ardından ABD'ye babasının yanına taşınmış ve bir teknoloji firmasında kısa süre çalışmıştır. Burada üvey annesi ile yaşadığı sorunlar nedeni ile çok barınamamış ve babasının arabasında evsiz olarak yaşamaya başlamıştır. 2006 yılında Chicago'da "evsiz bir hacker" hayatı sürmüş, bir süre sonra Maryland'deki teyzesinin evinde yaşamaya başlamıştır (Manning, 2022: 35–48).
Manning zor geçen Chicago döneminden sonra teyzesinin yanında kalırken Maryland'de üniversiteye yazılmış, yazılım becerilerini kullanacağı bir iş bulmak istemiş ama arşiv araştırmasından çekindiği için firmalara başvuru yapmamıştır. Manning bu dönemini anlatırken madde kullanımından, cinsiyet değiştirme amacıyla hormon tedavisi almak istemesinden ve bununla ilgili terapi aldığından bahsetmektedir. 2007 yılında çalışması gerektiği için üniversiteyi bırakmak zorunda kalmıştır. Kendi deyimiyle öncelikle "babasını saygısını kazanmak", cinsel

kimliği ile ilgili sorunlarını çözmek ve üniversite okuyabilmek amacıyla asker olmaya karar vermiştir (Manning, 2022: 49–54).

Manning Eylül 2007'de asker olmak için başvuru yaptığında aynı gün içinde hem yetenek ve akademik testlerini geçmiş hem de bu testlerin ardından verilerle çalışmak istediğini belirterek askerî analist olarak kaydolmuştur. Kendisinin de belirttiği gibi süreç çok hızlı ilerlemiş ve ordunun askere ihtiyacı olduğundan hemen kaydolması halinde 20.000 dolar bonus alacağını öğrenmiştir. İkinci gün fiziksel testler ve evrak işi ile ilgilenilmiştir. Bu noktada Manning arşiv araştırması için SF-86 denilen formu doldururken forma yazdığı adreslere ve kişilere gidilmesi halinde askere alınamayacağını hissetmiştir. Dahası bu süreçte evsiz olduğunu, uyuşturucu kullandığını, psikiyatriste gittiğini beyan etmesine rağmen, bunların sorun yaratmayacağı kendisine iletilmiştir. Nitekim bunlar sorun olmamış ve birkaç gün içinde temel askerî eğitim alacağı Missouri'de bulunan Fort Leonard Wood birliğine katılmıştır (Manning, 2022: 54–56).

Mannig'in asker olmadan önceki geçmişi; yaşadığı ailevi sorunlar temelli kimlik bunalımı, madde kullanımı, yasadışı eylemler, düzeniz bir hayat ile tanımlanabilir. Bu süreçte Manning'e dair somut işaretler mevcuttur fakat İKK'nın personel güvenliği ilkesi (özellikle arşiv araştırması safhası) ihlal edilmiş ve gizli bilgileri teslim edebilecek bir kişilik yapısına sahip olup olmadığı sorgulanmadan böyle bir pozisyon için askere alınmıştır.

**Sınıf Eğitimi Dönemi**

Temel askerî eğitimi tamamladıktan sonra Manning, istihbarat sınıfındaki askerlerin eğitim aldığı Sierra Vista'daki Fort Huachuca garnizonuna katılmıştır. Burada Manning, 24 hafta ve (haftada 50) saat istihbarat analizi üzerine eğitim almıştır. Kendi deyimiyle bu eğitimde "isyancılar gibi düşünmeyi, gerilla savaşçılarının neler yapabileceğini ve konvansiyonel dezavantajları konvansiyonel olmayan avantajlar olarak nasıl kullanabileceğini" öğrenmiştir. Eğitim sürecinde de cinsel kimliğini açıktan söylemese de bunu belli edecek şekilde davrandığını aktarmaktadır. Eğitimden arta kalan zamanlarında yalnızlık hissini gidermek amacıyla internet bağlantısına sahip laptopu ile Youtube, Facebook ve 4chan gibi sitelerde zaman geçirmiştir. Kendi ifadesiyle "rahat arkadaşça bir ortamda olmasına rağmen kendisini yalnız hissettiği ve askerî kültüre ve onun kuralcı erkekliğine yabancılaştığı iş yerinde alamadığını düşündüğü her şeyi sohbet odalarından" almıştır (Manning, 2022: 63–68).

Eğitim döneminde İKK'nın yönetim sorumluluğu ve gerçekçi politikalar ve prosedürler, yönetim desteği ilkelerinin ihlal edildiği anlaşılmaktadır. Askerî kültüre adapte olamayan bir personel uygulanmayan denetim ve İKK politikaları nedeniyle tespit edilememiştir.

**İstihbarat Analisti Dönemi**

Sınıf eğitimini tamamlamasının ardından Manning Ağustos 2008'den itibaren New York Fort Drum'da istihbarat analisti olarak çalışmaya başlamıştır. Buradaki işi Afganistan'daki askerlere istihbarat analizi üretmekti. Manning yaptığı işi sorgulamaya burada başlamıştır aslında. Kendi ifadesiyle "Hükümetin yararlandığı hassas yöntemlerle kişiler hakkında (ilişki kalıpları, kimlerle konuştukları, arkadaşlarının kimlerle konuştuğu, ne satın aldıkları, sırları, cinsellikleri, ihanetleri) her şeyi" öğrenebildiğini aktarmaktadır. Manning, mevcut bilgilerin derinliği ve genişliğinden etkilendiğini belirtmektedir. Bu dönemde eş zamanlı olarak Manning internette hoşlaşmadığı dini gruplara yönelik siber saldırı eylemlerine anonim olarak katılmayı sürdürmüştür. Bunun yanında Manning, kurum dışında tanıştığı gazetecinin birine ordunun o dönem cinsel konular hakkında takip ettiği "Don't ask, Don't Tell" politikası hakkında ve bu konuda iç işleyişin nasıl olduğu konusunda bilgiler ve gizlilik derecesi olmayan belgeler vermiştir (Manning, 2022: 64–78).

Manning ordudaki İKK zayıflıklarının da bu dönemde farkına varmaya başlamıştır. Analizimiz açısından doğrudan Manning'in kendi kaleminden İKK ilkelerinin nasıl ihlal edildiğine dair bilgiler önem taşımaktadır. Manning işinin bir parçası olarak silahlarla ve gizli bilgilerle dolu kasaların ve cephaneliklerin doğru fiziksel güvenlik önlemlerine sahip olduğundan emin olmakla ilgilenmektedir. Manning ordunun inanılmaz güvenlik riskleriyle dolu olduğunu kısa sürede fark ettiğini belirtmektedir. Örneğin, Manning üsteki ateşli silahlar kasasının (tüfeklerle ve devasa bir mühimmat deposuyla dolu) kilidi hala fabrika ayarlarına ayarlı olduğuna dikkat çekmektedir. Elektronik cihazların fiziksel güvenliğini sağlamak için muazzam miktarda enerji harcanmasına rağmen elektronik cihazların kendisinde güvenlik zaafiyeti olduğuna işaret etmektedir (gerçekçi politikalar ve prosdürler ilkesi, derinlikli savunma ilkesi ihlali). Manning, bu dönemde sistemin açıklarından yararlanarak erişim izni olmadığı veri tabanlarına girmeye başlamıştır. Hatta bazen üstlerinin bilgisi dahilinde kendi işleri için gerekli ama erişim izni olmayan verilere eriştiğini bildirmektedir. Kendi ifadesiyle bu konudaki "tek kural yakalanmamaktı". Bir keresinde büyük bir veri tabanını izinsiz bir alana aktarırken yanlışlıkla, tüm birliğin internet erişimini kesmiş ve verilerin kaybolmasına neden olmuştur. Yaptığı şeyi itiraf etmesine rağmen herhangi bir ceza almamıştır (Yönetim Sorumluluğu, Yönetim Desteği, Bilmesi Gerekenler, Gerçekçi Politikalar ve Prosedürler, Sinerjik Yaklaşım ilkelerinin ihlali) ( (Manning, 2022: 79–80).

Ekim 2009'da Manning Bağdat'ın 40 km doğusunda bulunan Amerikan üssüne (Forward Operation Base Hammer) görevlendirilmiştir. Burada çalışmaya başladıktan kısa bir süre sonra terfi almıştır. İstihbarat analisti olarak Manning, çok gizli, gizli ve tasnif dışı bilgiler ile çalışıyordu. Manning, bir noktada psikolojik olarak sorunlar yaşamaya başladı, kendi deyimiyle "simülasyonda yaşıyor" gibi hissetmiştir. Manning özellikle sahada gördükleriyle, basına yansıyanlar arasındaki farkı sorgular hale gelmişti. Yaşadığı kimlik karmaşası ve Irak'ta yaşananlara tanıklık etmesi Manning'te depresyon, anksiyete, öfke ve aşırı stres gibi sorunlara yol açınca, komutanı Manning'i terapiste yönlendirmiştir (Manning, 2022: 97–108).

Gizli bilgilere erişim kolaylığının anlaşılması için o dönemin İKK bağlamında tüm ABD kurumlarında yerleşen yanlış politikaların bilinmesi gerekmektedir. 11 Eylül sonrası sorunlardan biri olarak bilgi paylaşımı tespit edilmesiyle ABD kurumlarında istihbaratın katı hiyerarşik düzeni değişmiş, istihbarat paylaşımı Manning'in çalıştığı dönemde artmıştı. Aynı şekilde gizli belgelerin sayısı da 11 Eylül'den sonra katlanarak artmıştı. 2000 yılında yaklaşık sekiz milyon belge gizli olarak tasnif edilirken Manning'in çalıştığı dönemde yılda elli milyondan fazla gizli belge yeni istihbarat paylaşım politikasıyla kurumlar arasında dolaşıyordu. Manning çalıştığı yerdeki bilgi güvenliğinin de çok sağlam olmadığına dikkat çekmektedir. Manning'ten sözde yüksek güvenlikli ofislerinde insanların devlet sırlarını içeren dizüstü bilgisayarların şifrelerini aynı dizüstü bilgisayarlara yapıştırılmış ve post-it'lere yazılmış olarak sakladığını öğrenmekteyiz (Yönetim Sorumluluğu, Yönetim Desteği, Bilmesi Gerekenler, Gerçekçi Politikalar ve Prosedürler, Sinerjik Yaklaşım, Derinlikli Savunma ilkesi ihlali). Manning'in aktardığına göre insanlar SCIF'in herhangi bir odasında herhangi bir kişisel materyal bulundurulmasına karşı katı düzenlemeleri açıkça göz ardı ediyor ve herkes müzik, bilgisayar oyunları, kaçak filmler gibi şeyler için DVD kullanabiliyordu. Manning de kendi işi için gerekli olan belgeleri yedek olarak DVDlere kaydedebilmekteydi. Nitekim Manning 2010 yılbaşı gecesi "dünyayı değiştirmeye" karar verdikten sonra bu amaçla kullandığı DVD'leri SCIF'ten çıkarması hiç sorun olmadı çünkü o zamana kadar herkesin yaptığı bir eylemdi (Manning, 2022: 109–120).

Hikayenin geri kalanı zaten bilinmekte: Manning'in sızdırdığı bilgiler, The New York Times ve The Washington Post gibi büyük Amerikan gazetelerinde sık sık manşetlerde yer aldı. Yargılanmasının sonunda Manning, 1917 Casusluk Yasasını ihlal etmekten suçlu bulundu. Verilen otuz beş yıllık hapis cezası, ABD devletine ait bilgilerin sızdırılması ve bu bilginin kamuoyuna açıklanması amacıyla gerçekleştirilen bir davada o güne kadar verilen en uzun ceza olarak kayıtlara geçmiştir (Maxwell, 2018: 100).

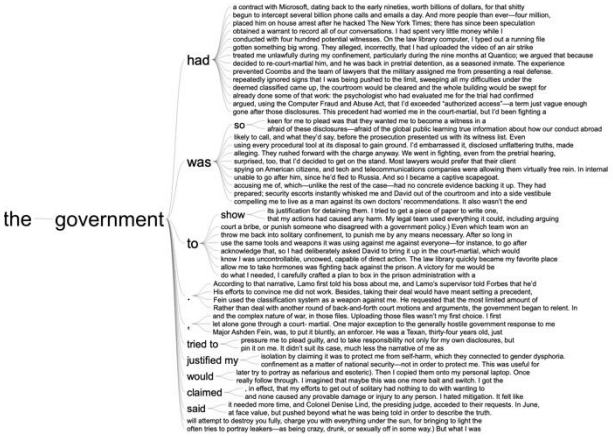
Manning'in sızıntılarına varan süreçte açıkça İKK ilkeleri ihlallerinin norm haline geldiği görülmektedir. Yönetim sorumluluğu, yönetim desteği, bilmesi gerekenler, gerçekçi politikalar ve prosedürler, sinerjik yaklaşım, erken tespit, derinlikli savunma, öngörülemezlik, nitelik ve nicelik, belirle ve önceliklendir ilkelerinin tamamı asker olarak çalıştığı dönemde ihlal edilmiştir. Bu nedenle Manning'in oluşturduğu tehdit caydırılamamış, tespit edilememiş ve engellenememiştir.

## İÇERİK ANALİZİ

Manning'in otobiyografisi nitel araştırma yöntemlerinde sıklıkla kullanılan Masqda programı kullanılarak analiz edilmiştir. İlk olarak otobiyografinin genel resminin çekilmesi amacıyla hangi kelimelerin ne sıklıkla otobiyografide kullanıldığı anlamak için kelime frekans analizi yapılmıştır (and, but gibi İngilizce'deki bağlaçlar ve was, did gibi tek başına anlam ifade etmeyen kelimeler göz ardı edilmiştir). Buna göre; en çok kullanılan kelimeler arasında öne çıkanlar şu şekildedir: People (halk, insanlar) 278 kez, government (hükümet) 164 kez, military (ordu) 157 kez, information (bilgi) 109 kez, army (ordu) 63 kez, security (güvenlik) 62 kez, public (kamu) 58 kez, intelligence (istihbarat) 42 kez kullanılmıştır.


**Şekil 1:** *Readme.txt* Kelime Bulutu

Kelime sıklık analizinin ardından en çok kullanılan kelimeler ve İKK açısından önemli olan kelimeler göz önünde bulundurularak "the government" (hükümet), "access" (erişim), "classified" (gizli), "security" (güvenlik), "intelligence" (istihbarat) kelimeleri seçilmiştir. Bu seçilen kelimeler Masqda programının kelime kombinasyonları özelliği ile analiz edilmiştir. Analiz sonuçlarına göre "the government kelimesi" en çok tried (denedi), justified (savundu), claimed (iddia etti) kelimeleri ile birlikte kullanılmıştır (Şekil 2.).




**Şekil 2**: "The government" Kelime Ağacı

Kelima ağacı analizi yöntemiyle analiz edilen ikinci kelime "access" kelimesidir. Analiz sonuçları "access" kelimesinin en çok "information" (bilgi) ve "hormones" (hormon) kelimeleri ile birlikte kullanıldığını göstermektedir (Şekil 3.)


**Şekil 3:**"Access" Kelime Ağacı

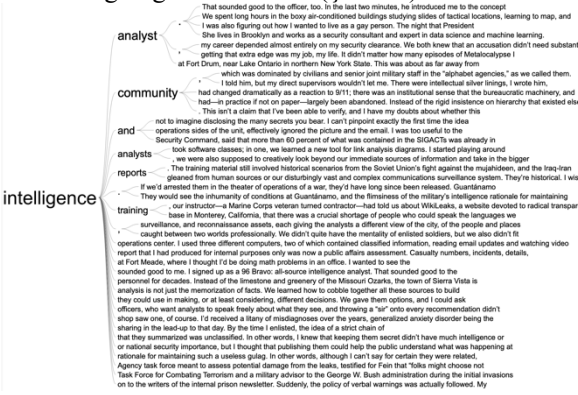
Üçüncü olarak ise "classified" kelimesi analiz edilmiştir. "Classified" kelimesi en çok "information" (bilgi), "documents" (belge), "network" (ağ) ve "material" (materyal) kelimeleriyle birlikte kullanılmıştır (Şekil 4.).


**Şekil 4:** "Classified" Kelime Ağacı

Dördüncü olarak "security" kelimesi kelime ağacı yöntemiyle analiz edilmiş ve kelimenin en çok"clearance" (yetki), "measures" (önlemler), "information" (bilgi") kelimeleri ile birlikte kullanıldığı ortaya koymaktadır (Şekil 5.).


**Şekil 5:** "Security" Kelime Ağacı

Son olarak ise "intelligence" kelimesi kelime ağacı yöntemiyle analiz edilmiş ve sonuçlar bu kelimenin en çok "analyst" (analist), "community" (topluluk), "reports" (rapor) ve "tranining" (eğitim) kelimeleri ile birlikte kullanıldığını göstermektedir (Şekil 6.).




**Şekil 6:** "Intelligence" Kelime Ağacı

## SONUÇ VE DEĞERLENDİRME

Manning vakası İKK açısından alınması gereken derslerle doludur. ABD istihbarat topluluğu açısından etkisinin büyüklüğü Ekim 2011'de yayınlanan Başkanlık Kararnamesi ile Ulusal İç Tehdit Görev Gücü'nun kurulmasından anlaşılabilir. Bu kararname ile Başkan, gizli ağlara sahip federal birimler ve kurumları iç tehdit tespit ve önleme programları oluşturmaya yönlendirmiştir (Natıonal Insider Threat Task Force (NITTF), n.d.). Vakanın gerçekleşme nedenlerinin başında gizli belgelere ve askerî ağa erişim sorunu gelmektedir (Hughes & Stoddart, 2012: 638). ABD Ulusal İstihbarat Direktörlüğü Bilgi Paylaşım Sorumlusunun da 2011 yılında konu ile ilgili Senatoda yaptığı konuşmada belirttiği üzere bilmesi gerekenler, bulunması gerekenler, derinlikli savunma başta olmak üzere İKK prensiplerinin neredeyse hiçbirisi bu durumda işe koyulmamıştır (Stone, 2011). Bunun nedeni resmî olarak ABD hükümeti tarafından onaylanmasa da, tahminlere göre yaklaşık "2,5 milyon ABD askeri ve sivil personel" SIPRNet'e erişim sağlayabilmesidir ("Siprnet: Where the Leaked Cables Came From," 2010) Nitekim Manning vakasının yaşanmasının ardından diplomatik yazışmaların SIPRNet'e yüklenmesi sonlandırılmıştır (Best, 2011).

Manning'in ağ erişiminin ve güvenlik izni olan en az 2,5 milyon diğer kişinin erişiminin bir istisna olarak değil, ağ toplumunda askerî çalışmanın tipik bir örneği olarak görülmesi gerekir. Nicks'in (2012) de belirttiği gibi, bu durumun normalliği, Manning'e devlet sırlarına benzeri görülmemiş erişim sağlamada rol oynamıştır (Nicks, 2012: 116). Otobiyografisine uygulanan kelime ağacı analizi sonuçları Manning'in gizli belgelere erişiminden bahsetme sıklığı açısından fikir vermektedir.

Erişim izni konusu İKK açısından bilmesi gerekenler açısından önemlidir. 2014 rakamlarına göre, ABD'de yaklaşık 4,5 milyon Amerikalı, yani toplam nüfusun yaklaşık %1,5'i, geçerli bir güvenlik iznine sahiptir. Daha özel olarak, bu rakam Personel Yönetim Ofisi'nin (OPM) sınıflandırmasına göre Tier 3 veya Tier 5 güvenlik iznine sahip bireyleri ifade etmektedir (2014 Report on Security

Clearance Determinations April 2015, 2015). Manning vakasından anlaşılacağı üzere en alt kademedeki bir güvenlik izni bile düzenli bir İKK programı olmadığında ve İKK ilkeleri ihlalleri yaşandığında büyük sorunlara yol açabilmektedir.

İKK açısından Manning vakasına has sorunlar askere alım ile başlamaktadır. İçerik anakizi ve kelime analizlerinden de görüldüğü üzere kimlik sorunları olan ve bunun için terapi almış, bir dönem evsiz olarak sokaklarda yaşamış, madde kullanmış bir kişinin tahkikatı hakkıyla yapılmamış gözükmektedir. Bundan daha önemli olan ise Manning bu sorunları hakkındaki kaygılarını doğrudan işe alım personeline iletmiş fakat bunlar dikkate alınmayarak Manning askere kabul edilmiştir. Savaş dönemi gibi kriz zamanlarında ortaya çıkan personel ihtiyacının bu duruma neden olduğu açıktır. Fakat İKK'nın niteliği niceliğe tercih etme ilkesi doğrultusunda istihbarat analisti gibi önemli bir pozisyonda çalışacak personel için böylesi bir geçmiş sorun olarak algılanmalıdır.

Manning'in anlattıkları Fort Drum ve Irak'taki üslerde İKK açısından büyük güvenlik zafiyetlerini de ortaya koymaktadır. Özellikle güvenlik kelimesinin kullanım sıklığı ve kelime ağacı sonuçları ve Manning'in belirgin bir şekilde fiziksel bariyerlerin olmayışı, şifrelerin fabrika ayarlarında veya açık olarak etrafta oluşundan doğrudan bahsetmesi İKK'nın özellikle yönetim sorumluluğu, yönetim desteği, bilmesi gerekenler, gerçekçi politikalar ve prosedürler, sinerjik yaklaşım, erken tespit, derinlikli savunma, öngörülemezlik, nitelik ve nicelik, belirle ve önceliklendir ilkelerinin ihlal edildiğini göstermektedir.

Buradan anlaşılmaktadır ki yanlış veya yapılmaması gerekenlerin hepsi norm şeklini almış ve Manning gibi iç tehditlerin işini kolaylaştıracak şekilde bir caydırıcılık sağlayamamıştır. Bunun yanında Manning daha Irak'a görevlendirilmeden önce çalıştığı Fort Drum üssünde de erişim izni olmadığı verilere erişmiş, bundan üstlerinin haberi olmasına rağmen kendi işlerini kolaylaştırdığı için Manning cezalandırılmamıştır. Böylesi bir çalışma ortamı ve davranış örüntüsü nihayetinde bu büyük sızıntılara giden yolun kolaylaştırıcıları olarak gözükmektedir. İKK ilkelerinin ihlalleri bir iç tehdidin öngörülememesi ve tespit edilememesiyle sonuçlanmıştır. Bu öngörülemeyen iç tehdit daha fazla veriye erişim sağlayabileceği, savaş ortamı ve tehdidin kimlik sorunları düşünüldüğünde tam bir risk kaynağı olarak daha kırılgan ve öngörülemez bir hal alacağı bir birliğe görevlendirilmiştir. Burada da neredeyse tüm İKK ilkeleri atlanarak savunmasız kalınmış ve "bilginin özgür olmasına" inanan ve kimlik bunalımları yaşayan fanatik bir iç tehdide dönüşen Manning tarihin en büyük sızıntısına neden olmuştur. Bu süreçte İKK açısından ihlal edilen ilkeler Tablo 1.'de görülmektedir.

**Tablo 1:** İhlal Edilen İlkeler ve Dönemler

| İlkeler | Asker olmadan önce | Eğitim Dönemi | İstihbarat Analisti Dönemi |
|---|---|---|---|
| Yön. Sorum. | | X | X |
| Yön. Desteği | | X | X |
| Etik | | | |
| Bul.Gereken. | | | X |
| Bil. Gereken. | | | X |
| Keşfe K.K. | | | |
| Gerçekçi Pol. | | X | X |
| Sin.Yak. | | | X |
| Erken Tes. | | | X |
| Der.Sav. | | | X |
| Öngörülemez. | | | |
| Kor.Gereken. | | | |
| Bel.ve Ön. | | | X |
| Nit. ve Nic. | | | X |
| İş Birliği | | | |
| Teh.Az. | | | |
| Per.Güven. | X | | |

Vaka üzerinden yapılacak İKK çalışmaları teori ile pratiği birleştirilmesine ve örnek olaylar ile alınması gereken derslerin somutlaşmasına katkı sağlamaktadır. Bu nedenle bu alanda vaka çalışmaları devam etmeli, tarihte yaşanan vakalar teorik temelli ve nitel araştırma yöntemleriyle ele alınmalıdır. Bunun yanında Manning vakası motivasyonu itibariyle Manning'in hapishaneden çıktıktan sonraki röportajları, söylemleri ve tutumlarıyla da çalışılarak İKK açısından analiz edilmelidir.

## KAYNAKÇA

2014 Report on Security Clearance Determinations April 2015. (2015), Office of The Director Of National Intelligence. https://www.dni.gov/files/documents/2015-4-21%20Annual%20Report%20on%20Security%20Clearance%20Determinations.pdf

Ball, J. (2011), WikiLeaks publishes full cache of unredacted cables. The Guardian. https://www.theguardian.com/media/2011/sep/02/wikileaks-publishes-cache-unredacted-cables

Bellia, P. L. (2012), WikiLeaks and the Institutional Framework for National Security Disclosures. Yale Law Journal, 121, 1448–1526.

Best, R. A. (2011), Intelligence Information: Need to Know vs. Need to Share. https://sgp.fas.org/crs/intel/R41848.pdf

Cole, L. (2022), Intelligence Collection and Ethical Behavior in the Post 9/11 Era, Doktora Tezi, Monarch Business School Switzerland.

Davies, N., & Leigh, D. (2010), Afghanistan war logs: Massive leak of secret files exposes truth of occupation. The Guardian. https://www.theguardian.com/world/2010/jul/25/afghanistan-war-logs-military-leaks

Entman, R. M., Matthes, J., & Pellicano, L. (2009), Nature, sources, and effects of news framing. In K. Wahl-Jorgensen & T. Hanitzsch (Eds.), The handbook of journalism studies, 175–190, Routledge.

Explosive Leaks Provide Image of War from Those Fighting It. (2010), Spiegel International. https://www.spiegel.de/international/world/afghanistan-explosive-leaks-provide-image-of-war-a-708314.html

Gioe, D. V. (2014), Tinker, Tailor, Leaker, Spy. The National Interest, 129, 51–59.

Greatest Data Leak in US Military History. (2010), Spiegel International. https://www.spiegel.de/international/world/the-wikileaks-iraq-war-logs-greatest-data-leak-in-us-military-history-a-724845.html

Hartline, C. L., Jr. (2017), Examination of Insider Threats: A Growing Concern, Yüksek Lisans Tezi, Utica College.

Hayden, M. (1999), The Insider Threat to U.S. Government Information Systems. National Security Agency. https://nsarchive.gwu.edu/sites/default/files/documents/3460882/Document-05-Michael-Hayden-National-Security.pdf

Hughes, R. G., & Stoddart, K. (2012), Hope and Fear: Intelligence and the Future of Global Security a Decade after 9/11. Intelligence and National Security, 27:5, 625–652.

Hunt, E. (2019), The WikiLeaks Cables: How the United States Exploits the World, in Detail, from an Internal Perspective, 2001–2010. Diplomacy & Statecraft, 30:1, 70–98.

Irak: L'horreur ordinaire révélée par Wikileaks. (2010), Le Monde. https://www.lemonde.fr/proche-orient/article/2010/10/22/irak-l-horreur-ordinaire-revelee-par-wikileaks_1429990_3218.html

Jensen III, C. J., McElreath, D. H., & Graves, M. (2018), Introduction to intelligence studies. Routledge.

Johnson, L.K. (2006), National Security Intelligence. In L.K. Johnson (Eds.), The Oxford Handbook of National Security Intelligence, Oxford University Press, 3-32.

Konstantopoulos, I. L. (2017), Democracy and Ethics vs. Intelligence and Security: From WikiLeaks to Snowden. In G. C. Bitros & N. C. Kyriazis (Eds.), Democracy and an Open-Economy World Order, 3–23, Springer International Publishing : Imprint: Springer.

Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., & Osula, A.-M. (2015), Insider Threat Detection Study. NATO Cooperative Cyber Defence Centre of Excellence.

La verdad sobre el "Cablegate." (2010), El Pais. https://elpais.com/internacional/2010/12/04/actualidad/1291417217_850215.html

Las dos filtraciones masivas que revelaron el detalle íntimo de la guerra. (2010), El Pais. https://elpais.com/internacional/2010/11/28/actualidad/1290898802_850215.html

Levine, A. (2010), Gates: Leaked documents don't reveal key intel, but risks remain. CNN. https://edition.cnn.com/2010/US/10/16/wikileaks.assessment/index.html

Los crímenes de Irak se revelan al mundo. (2010), El Pais. https://elpais.com/diario/2010/10/24/internacional/1287871201_850215.html#

Lowenthal, M.(2020), Intelligence From Secrets to Policy (Eight Edition). Sage

Luckey, D., Stebbins, D., Orrie, R., Rebhan, E., Bhatt, S. D., & Beaghley, S. (2019), Assessing continuous evaluation approaches for insider threats: How can the security posture of the U.S. departments and agencies be improved? RAND Corporation.

Manning, C. (2022), README.txt: A memoir (First edition). Farrar, Straus & Giroux.

Maxwell, L. (2018), Whistleblower, Traitor, Soldier, Queer?:The Truth Of Chelsea Manning. The Yale Review, 106:1, 97–107.

Montgomery, A. E. (2012), Organizational culture's effects on information sharing within the United States Intelligence Community,Yüksek Lisans Tezi, Georgetown University.

Natıonal Insider Threat Task Force (NITTF). (t.y.). The National Counterintelligence and Security Center. https://www.dni.gov/index.php/ncsc-features/243-how-we-work/1449-national-insider-threat-task-force-nitff

Ndeley, M. E. (2013), The Effect Of Wikileaks On Freedom Of Expression Globally, Yüksek Lisans Tezi, University Of Johannesburg.

Nicks, D. (2012), Private: Bradley Manning, Wikileaks, and the biggest exposure of official secrets in American history (1st ed). Chicago Review Press.

Prunckun, H. (2019), Counterintelligence theory and practice (Second edition). Rowman & Littlefield.

Randal, M. (2011), Propaganda and the Ethics of WikiLeaks. Global Media Journal: Australian Edition, 5:1, 1–8.

Roberts, A. (2012), WikiLeaks: The illusion of transparency. International Review of Administrative Sciences, 78:1, 116–133.

Sifry, M. L. (2011), Wikileaks and the age of transparency. O/R Books.

Siprnet: Where the leaked cables came from. (2010), BBC. https://www.bbc.com/news/world-us-canada-11863618

Stone, C. R. (2011), Statement for the Record before the Senate Homeland Security and Governmental Affairs Committee: 'Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration'. Office of the Director of National Intelligence. https://apps.dtic.mil/sti/pdfs/ADA539585.pdf

The National Counterintelligence and Security Center. (t.y.), National Insider Threat Task Force Mission Fact Sheet. https://www.dni.gov/files/NCSC/documents/products/National_Insider_Threat_Task_Force_Fact_Sheet.pdf

Thorsen, E., Sreedharan, C., & Allan, S. (2013), WikiLeaks and Whistle-blowing: The Framing of Bradley Manning. In B. Brevini, A. Hintz, & P. McCurdy (Eds.), Beyond WikiLeaks: Implications for the future of communications, journalism and society, 101–122, Palgrave Macmillan.

Ünsal, A. (2021), "Whistleblowing" Kavramının Türkçe'ye Aktarımında Asemantik Sorunların Meta Etik Analizi Ve Bir Semantik Öneri. Journal of International Management, Educational and Economics Perspectives, 9:2, 188–196.

Vrist Ronn, K. (2016), Intelligence Ethics: A Critical Review and Future Perspectives. International Journal of Intelligence and CounterIntelligence, 29:4, 760–784.

WikiLeaks Diplomatic Cables. (2010), Spiegel International. https://www.spiegel.de/thema/wikileaks_diplomatic_cables_en/p6/

WikiLeaks embassy cables: The key points at a glance. (2010). The Guardian. https://www.theguardian.com/world/2010/nov/29/wikileaks-embassy-cables-key-points

Wikileaks évoque des "preuves de crimes de guerre" dans les rapports sur l'Afghanistan. (2010), Le Monde. https://www.lemonde.fr/asie-pacifique/article/2010/07/26/wikileaks-evoque-des-preuves-de-crimes-de-guerre-dans-les-rapports-sur-l-afghanistan_1392346_3216.html

WikiLeaks publie l'intégralité des 250 000 câbles diplomatiques américains. (2011), Le Monde. https://www.lemonde.fr/technologies/article/2011/09/02/wikileaks-publie-l-integralite-des-250-000-cables-diplomatiques-americains_1566648_651865.html

## EXTENDED ABSTRACT

In 2010, one of the biggest leaks in world history occurred through Wikileaks. Private Bradley Manning, while serving as a military intelligence analyst in Iraq, leaked approximately 750,000 documents to Wikileaks. The question of how a military intelligence personnel of the rank of private could cause a leak of this magnitude is the main focus of this study. Hence, the Manning case, which can be categorized as an internal threat, is important in terms of lessons to be learned in terms of counter-intelligence (CI). This study analyzes the Manning case from the point of view of CI based on her autobiography (Readme.txt). The study reveals that all the principles of CI were violated from the personnel investigation process until the time of the leak.

The Manning case is full of lessons for the CI. The magnitude of its impact on the US intelligence community can be seen in the establishment of the National Insider Threat Task Force by Presidential Decree in October 2011. The President directed federal departments and agencies with classified networks to establish domestic threat detection and prevention programs. One of the main reasons for the incident was the problem of access to classified documents and the military network. As Intelligence Community Information Sharing Executive Office of the Director of National Intelligence stated in his 2011 Senate testimony on the subject, almost none of the principles of the CI - need-to-know, need-to-be, defense-in-depth - were put to work in this case. This is because, although not officially confirmed by the US government, it is estimated that around 2.5 million US military and civilian personnel had access to SIPRNet. Indeed, after the Manning case, the uploading of diplomatic correspondence to SIPRNet was terminated.

Manning's network access, and that of at least 2.5 million others with security clearance, should not be seen as an exception, but as typical of military work in a network society. The normality of this situation played a role in giving Manning unprecedented access to state secrets. The issue of access authorization is also important for those who need to know about it. According to 2014 figures, approximately 4.5 million Americans in the US, or about 1.5% of the total population, have a valid security clearance. More specifically, this figure refers to individuals with a Tier 3 or Tier 5 security clearance according to the Office of Personnel Management (OPM) classification. Even the lowest tier security clearance can cause major problems in the absence of a regular CI program.

In terms of CI, the problems specific to the Manning case begin with recruitment. It seems that a person with identity issues, who had received therapy for this, who had lived on the streets as a homeless person for a while, and who had used substances, was not properly investigated. More importantly, Manning communicated his concerns about these issues directly to the recruitment staff, but they were ignored and Manning was accepted into the army. It is clear that the need for personnel in times of crisis, such as wartime, is the cause of this situation. However, in line with the CI's principle of preferring quality over quantity, such a background should be perceived as a problem for personnel who will work in an important position such as an intelligence analyst.

Manning's account also reveals major security weaknesses in terms of the CI at Fort Drum and the bases in Iraq. The lack of physical barriers, the passwords being in factory settings or openly lying around have become commonplace, contrary to all the principles of the CI. Everything that is supposed to be wrong or should not be done became the norm and failed to provide a deterrent that would facilitate the work of internal threats like Manning. In addition, Manning accessed data that he was not authorized to access at Fort Drum, where he worked before he was deployed to Iraq, and although his superiors were aware of this, Manning was not punished for facilitating their work. Such a working environment and behavioral pattern ultimately appear to be the facilitators of the path to these major leaks. The failure to adopt a realistic CI policy resulted in the failure to anticipate and detect an internal threat. The unforeseen insider threat was assigned to a unit where it could gain access to more data and where the war environment would make the threat more vulnerable and unpredictable given its identity issues. Here, too, all the principles of the CI were bypassed and Manning, who believed in the "freedom of information" and turned into an internal threat with identity crises, caused the biggest leak in history.